

POSITION PAPER

Committee: United Nations Human Rights Council

Country: Germany

Agenda: Human Rights Implications of Mass Digital Surveillance During Political Protests and Civil Unrest

Introduction

The Federal Republic of Germany affirms that peaceful protest is a central expression of democratic participation and political accountability. Under Article 5 of the Basic Law for the Federal Republic of Germany, every person has the right to freely express and disseminate opinions and to obtain information from generally accessible sources, while Article 10 protects the privacy of correspondence, posts, and telecommunications. Article 1 further establishes that human dignity is inviolable. Together, these provisions reflect Germany's view that democratic legitimacy depends on an open civic space in which citizens may speak, assemble, and access information without unjustified state intrusion.

Germany recognizes that states have a legitimate duty to protect public order and respond to genuine threats to security. Yet this responsibility is constrained by law and by the requirement that any interference with rights satisfy legality, necessity, proportionality, and independent review. This principle is not abstract: the Federal Constitutional Court has limited surveillance powers in multiple decisions, including its 2020 judgment on the Federal Intelligence Service's surveillance powers, its 2024 order on strategic telecommunications surveillance, and its 2024 ruling on certain Federal Criminal Police Office data-collection and retention powers. Germany therefore approaches this agenda from the position that security and rights are not opposing values, but jointly necessary conditions of a democratic state.

The increasing use of digital surveillance tools during protests and unrest has heightened the stakes of this debate. AI-based analytics, biometric identification, and communications monitoring can enable states to track dissent at scale, but they also create serious risks to privacy, free expression, and peaceful assembly. The Universal Declaration of Human Rights protects privacy, freedom of expression, and peaceful assembly in Articles 12, 19, and 20, while the International Covenant on Civil and Political Rights protects the same rights in Articles 17, 19, and 21. Germany considers these instruments foundational to any lawful approach to protest-related surveillance.

Background of the Issue

Mass digital surveillance refers to the collection, analysis, or retention of communications, metadata, location data, online activity, or biometric information, often at scale and without individualized suspicion. In the context of political protests, this may include monitoring social media, intercepting communications, tracking devices, deploying facial recognition systems, or using AI to identify participants, organizers, or networks of association. Such practices are especially sensitive because they are often directed at people engaged in lawful civic activity rather than criminal conduct.

The human rights consequences are substantial. Article 12 of the UDHR and Article 17 of the ICCPR prohibit arbitrary interference with privacy, while Article 19 of the UDHR and ICCPR protect the right to seek, receive, and impart information. Article 20 of the UDHR and Article 21 of the ICCPR protect peaceful assembly. Surveillance that is broad, opaque, or indefinite can chill all three rights at once by making people fear that lawful participation will lead to profiling, retaliation, or detention. Germany therefore considers transparency, oversight, and effective remedy indispensable in protest-related surveillance policy.

The digital environment also introduces new forms of risk through AI and facial recognition. The EU AI Act establishes a risk-based framework for AI governance, including stricter requirements for high-risk and certain biometric applications. This framework is particularly relevant to protest surveillance, where technologies may be used to classify individuals, infer behavior, or enable remote biometric identification. Germany supports this approach because biometric and AI systems must not be normalized in civic spaces without strict legal limits.

At the same time, Germany recognizes that serious unrest can involve violence, sabotage, or threats to life and infrastructure. In such cases, states may adopt targeted security measures. However, the existence of a legitimate aim does not dispense with rights obligations. Under both constitutional and international law, any interference must remain necessary, proportionate, and subject to review by an independent authority. Blanket restrictions, generalized monitoring, and unrestricted emergency powers are incompatible with democratic governance.

Germany's Position

Germany's position is anchored in the constitutional principle of human dignity under Article 1 of the Basic Law, which serves as the foundation of the entire legal order. Because dignity is inviolable, state action affecting protest, speech, or private communications must be directed toward persons as rights-holders protected by law. Article 5 then guarantees freedom of expression and access to information, while Article 10 safeguards the privacy of telecommunications. Together, these provisions establish that surveillance cannot be treated as a default tool of governance, particularly in contexts where political dissent is lawful.

Germany further holds that constitutional surveillance power must be narrowly framed and consistently supervised. The Federal Constitutional Court's recent jurisprudence confirms that even where security interests are real, the state may not impose surveillance powers that are overbroad or disproportionate. In 2020, the Court held that parts of the Federal Intelligence Service's foreign telecommunications surveillance regime violated the Basic Law; in 2024, it again found parts of strategic surveillance powers incompatible with Article 10(1); and in 2024 it also held that certain BKA data-collection and retention powers were unconstitutional in part. This jurisprudence demonstrates Germany's commitment to judicially enforceable limits on state intrusion.

Germany also treats data protection as a democratic safeguard. The General Data Protection Regulation protects personal data through principles such as lawfulness, purpose limitation, data minimization, storage limitation, integrity and confidentiality, and accountability. Individuals further have rights of access, rectification, erasure, restriction, objection, and complaint under the GDPR. Germany supports this framework because the protection of personal data is not merely administrative compliance; it is a condition for free political participation and trust in public institutions.

Germany's support for the EU AI Act follows the same logic. The Act establishes a European legal framework for AI governance and reflects the view that sensitive technologies require prior governance rather than retrospective correction. Germany considers this especially important for facial recognition and other biometric tools used in protest contexts, where the risk of error, abuse, and discriminatory impact is particularly high.

National Actions

Germany's domestic legal order already incorporates multiple safeguards relevant to this agenda. The Basic Law protects freedom of expression, information, assembly, and telecommunications privacy, while the Federal Data Protection Act supplements GDPR implementation in the national context. Germany's data protection system includes the Federal Commissioner for Data Protection and Freedom of Information (BfDI), which provides oversight and complaint mechanisms for federal data processing. These institutions ensure that rights violations can be challenged through lawful procedures rather than political appeal alone.

German courts remain a central check on surveillance excess. The Federal Constitutional Court has repeatedly required that surveillance powers be precisely defined, limited in purpose, and proportional to the legitimate aim

pursued. The Court's surveillance jurisprudence is especially relevant to protest monitoring because it demonstrates that security is not a constitutional blank cheque. Germany's legal order therefore prioritizes judicial authorization, transparent legal bases, and oversight mechanisms over broad executive discretion.

Germany also maintains a mature data protection enforcement structure. The BfDI's complaint procedure allows individuals to challenge unlawful processing, while supervisory authorities can investigate breaches and require corrective action. This matters in the surveillance context because the availability of effective remedy is essential to the meaningful enjoyment of rights. Without complaint, review, and enforcement, privacy and expression protections remain merely formal.

International Actions

Germany's position is fully consistent with its obligations under international human rights law. The UDHR protects privacy, expression, and peaceful assembly in Articles 12, 19, and 20, while the ICCPR protects the same rights in Articles 17, 19, and 21. These rights are not suspended simply because a state declares a public emergency; rather, any restriction must still satisfy the applicable legal standard, including legality and proportionality, and must remain compatible with democratic principles. Germany therefore supports a rights-based interpretation of emergency governance that does not normalize mass surveillance.

Germany also works through European legal frameworks to strengthen digital rights. The GDPR provides a region-wide model for accountability in personal data processing, while the EU AI Act addresses risks posed by high-risk AI systems, including biometric and other sensitive applications. Germany supports these tools because they allow states to preserve security while maintaining public trust and legal certainty. Germany sees its role as both implementing these standards domestically and promoting them internationally as part of a credible democratic model.

Within multilateral forums, Germany supports the UN Human Rights Council's role in setting norms around digital rights, surveillance, and civic space. Germany favors international cooperation on technical assistance, judicial capacity-building, information sharing, and cross-border privacy standards. Because surveillance technologies often operate across jurisdictions, Germany considers multilateral coordination essential to accountability. This includes support for rule-of-law institutions, privacy safeguards, and responsible AI governance.

Challenges

One major challenge is the speed of technological development. AI-enabled surveillance, biometric identification, and data analytics can be deployed faster than legal systems can adapt. This creates a governance gap in which intrusive tools may be used before clear standards, oversight, or remedy are in place. Germany therefore believes that prevention, not just post hoc accountability, must guide international responses.

A second challenge is cross-border surveillance and information sharing. Communications data may be processed outside the state where the protest occurs, while intelligence cooperation can obscure responsibility. This makes transparency, data-transfer safeguards, and independent oversight even more important. Germany considers cross-border privacy standards essential because rights protections lose force if they stop at the border.

A third challenge is digital authoritarianism, where protest surveillance, censorship, and communications restrictions are combined to suppress legitimate civic participation. In such settings, citizens may self-censor or avoid assembly altogether. Germany is concerned that this model not only violates rights but also undermines the legitimacy of state institutions by treating peaceful citizens as security objects rather than democratic participants.

Germany's Proposed Solutions

Germany proposes that states adopt clear statutory thresholds for protest-related surveillance. The objective is to ensure that intrusive monitoring is used only for a legitimate aim, when necessary and proportionate, and only under a clear legal basis. Implementation should rely on domestic legislation, judicial authorization where appropriate, and independent oversight by data-protection or constitutional bodies. The expected impact would be a reduction in arbitrary surveillance and a stronger framework for legal certainty. The main challenge will be balancing fast-moving security concerns with the need for procedural safeguards.

Germany also supports a strong presumption against blanket internet shutdowns. The objective is to preserve access to information, emergency communication, and lawful civic participation during unrest. Implementation should require a specific legal basis, transparent justification, temporal limits, and independent review. Responsible stakeholders include national legislatures, courts, telecom regulators, and human-rights oversight bodies. The expected impact would be to reduce collective punishment and protect democratic participation. The primary challenge is that states may claim broad emergency necessity; Germany's response is that necessity does not eliminate proportionality.

Germany further recommends strict governance for AI and facial recognition in protest settings. The objective is to prevent mass identification and profiling of peaceful demonstrators. Implementation should include risk assessments, procurement controls, purpose limitations, and, where appropriate, restrictions on real-time biometric identification in public assembly settings. The EU AI Act provides the strongest regional baseline for this work, and Germany supports its careful application. The expected impact would be lower misuse risk, reduced discrimination, and greater public confidence. The challenge is enforcement, especially where technologies are deployed through private vendors or cross-border systems.

Germany also supports stronger transparency and complaint mechanisms. The objective is to ensure that surveillance practices can be challenged and reviewed. Implementation should require public reporting, retention limits, notification rules where compatible with security needs, and access to supervisory authorities and courts. The responsible stakeholders are data-protection authorities, courts, and relevant ministries. The expected impact would be improved accountability and stronger public trust. The challenge is protecting sensitive operational information while still ensuring meaningful disclosure.

Finally, Germany supports international norm-building on digital rights during unrest. The objective is to establish common standards based on legality, necessity, proportionality, transparency, and effective remedy. Implementation should occur through the UN Human Rights Council, technical assistance programs, judicial cooperation, and cross-border privacy dialogue. The expected impact would be stronger global expectations and a more coherent rights framework. The challenge is achieving broad state consensus, especially where some governments prefer flexible emergency powers.

Conclusion

Germany believes that human rights protections during protests and civil unrest are not obstacles to security, but foundations of democratic legitimacy. States may respond to genuine threats, but they must do so within the bounds of law and respect for fundamental freedoms. Germany therefore rejects the normalization of mass digital surveillance, blanket restrictions on connectivity, and the misuse of emerging technologies against peaceful citizens. Its position is clear: a democratic state earns trust through restraint, accountability, and respect for human dignity.

Sources Used

- Basic Law for the Federal Republic of Germany, Articles 1, 5, and 10.
- Federal Constitutional Court decisions on surveillance and data retention.
- Federal Data Protection Act and BfDI oversight/complaints framework.
- General Data Protection Regulation.
- EU AI Act.
- Universal Declaration of Human Rights, Articles 12, 19, and 20.
- International Covenant on Civil and Political Rights, Articles 17, 19, and 21.